FLIGHT GUARDIAN: A COMMON AVIONICS ARCHITECTURE FOR COLLISION AVOIDANCE AND SAFE EMERGENCY LANDING FOR UNMANNED AERIAL SYSTEMS

Luis Mejias, Duncan Greer
Australian Research Centre for Aerospace Automation.
Queensland University of Technology. Brisbane. QLD. Australia

Abstract

This paper presents an approach to derive requirements for an avionics architecture that provide onboard sense-and-avoid and autonomous emergency forced landing capabilities to a UAS. The approach is based on two design paradigms that (1) derive requirements analyzing the common functionality between these two functions to then derive requirements for sensors, computing capability, interfaces, etc. (2) consider the risk and safety mitigation associated with these functions to derive certification requirements for the system design. We propose to use the Aircraft Certification Matrix (ACM) approach to tailor the system Development Assurance Levels (DAL) and architecture requirements in accordance with acceptable risk criteria. This architecture is developed under the name *"Flight Guardian"*. *Flight Guardian* is an avionics architecture that integrates common sensory elements that are essential components of any UAS that is required to be dependable. The *Flight Guardian* concept is also applicable to conventionally piloted aircraft, where it will serve to reduce cockpit workload.

Introduction

Operators who wish to deploy UAS for civilian applications currently face a significant challenge: regulations that define the operational and technical requirements are not yet in place and thus UAS cannot be fully integrated into the NAS. Not only has the technology to achieve integration not yet been developed, but the performance standards have also not yet been agreed upon. Without a clear set of performance standards, neither the potential benefits that civil UAS bring to society, nor the market expansion that has been predicted, will be realised. In this paper, we address the functional and certification requirements for two critical UAS capabilities – sense-and-avoid and automated emergency landing- in a unified architecture.

Yet with a regulatory framework, the widespread adoption of UAS in civilian contexts will be dictated by the design efficiency and cost reduction in their manufacturing. Which in turn has a significant impact in UAS dependability. The notion of a "Dependable UAS" is one in which the user can trust the UA system to perform its intended job without undue risk to themselves, the air vehicle, or third parties. The Dependable UAS is also one in which the user does not require an exceptional level of skill or experience in order to operate it safely.

In adopting dependability as a critical requirement, UAS system designers are also faced with the need to respond quickly to niche markets (i.e. changes in mission & payload requirements) without compromising safety, robustness and cost. Therefore, there is a need to amortize development cost by maximizing reusability and modularity in avionics that can be used across several platforms, and more importantly be reconfigured to accommodate specific missions. One way to achieve this is to design avionics architectures that take advantage of common sensors, interfaces and onboard computing.

In this paper, we propose an avionics architecture called "*Flight Guardian*" based on two critical onboard functions: (1) the ability to "sense and avoid" other aircraft, and (2) the ability to conduct a safe landing in case of an emergency. These two functions have been identified as two of the most critical technological barriers to the integration of UAS into the NAS [1, 2]. The design of such architecture is approached from two perspectives. Our initial approach to the problem is to consider the common functionalities between these two critical tasks to then derive requirements for sensors, computing capability, interfaces, etc. A common avionics architecture that adopts elements of

modularity and dependability can be shared between the required aircraft functions, leveraging common interface, processing and sensing elements. This will significantly reduce cost, equipment footprint and improve avionics supportability & maintenance. Additionally, we consider the risk and safety mitigation associated with these functions to derive certification requirements for the system design. We propose to use the Aircraft Certification Matrix (ACM) approach to tailor the system Development Assurance Levels (DAL) and architecture requirements in accordance with acceptable risk criteria.

Flight Guardian aims to be standards based, and improve the dependability of the UAS by removing the need for the user to closely monitor the environment around the aircraft, allowing them instead to concentrate on the mission results, and allowing the UA to operate safely in airspace with other airspace users, and over urban areas.

Dependability in UAS

The fundamental paradigm in designing the Dependable UAS is that safety is inherent in the air vehicle. That is, that continued safe flight and landing should be independent of any external system or signal. This is the principal that underpins conventional aviation, and unmanned systems should be no different. The definition of dependability that has been adopted by the authors is based the Laprie model [3, 4] from the computer science literature. That is that dependability is the property of a system that leads to the degree of trust that a user can place in the system to perform its intended function without causing undue hazards to itself, its users or its environment.

The Laprie model proposes that attributes of a dependable system are availability, reliability, safety, confidentiality, integrity and maintainability. The model also introduces the impairments to achieving dependability (faults, errors and failures), and means of achieving dependability (fault prevention, tolerance, removal and forecasting). The attribute of dependability that this paper is concerned with is safety. Safety of a system (in this case a UAS) is the ability of that system to operate without causing adverse consequences to its environment. Safety should not be confused with reliability – i.e a highly reliable system is not necessarily a safe one, even though the probability of an unsafe event occurring may be reasonably low.

There are many methods of achieving safety in an air vehicle system. We propose that *Flight Guardian* falls into two classes: fault prevention (i.e. prevent collisions with other aircraft), and fault tolerance (i.e. given that a particular failure has occurred, attempt to land the aircraft without causing any further damage). The dependability objectives of *Flight Guardian* will be achieved by adopting accepted aircraft development standards for the development assurance process which is discussed in detail later in this paper.

Two critical UAS capabilities

In this section we introduce the functional requirements of the sense-and-avoid and automated emergency landing systems, and consider the requirements they define for the onboard avionics.

Sense and avoid

Sense and avoid (SAA) is a necessary function of any aircraft system. There are many possible implementation architectures, which may include a combination of ground-based and aircraft-based sensors. We only consider aircraft-based systems for dependable UAS systems, since any failure of data links or ground-based infrastructure should not reduce the margins of safety of the air vehicle. Furthermore, onboard self-contained, passive, SAA systems have the capability to address non-cooperative[1] scenarios at the same it provide an alternative to the Size, Weight and Power (SWaP) limitations of many small-medium size UAS. A secondary function of the sense-and-avoid system is to keep any human operator aware of the system status, and of any actions taken by the system. This function, including the role of any human operator, is discussed in [5].

Sense-and-avoid begins with the detection of potential conflicting air traffic, and as a result considerable research and development has been dedicated to addressing the “sensing” aspect of sense-

[1] Cooperative implies that all vehicles in the air share information through common communication links. Uncooperative denotes the issue that vehicles in the sky are not communicated to each other, and therefore implies that there is not other way to detect other vehicles than a self-contained onboard sensor

and-avoid. An important design choice in the development of sensing and detection systems is the type of sensor used to collect information about the surrounding environment, and the cooperative or uncooperative nature of the system. This is a choice that must account for the physical and resource limitations of the UAS , and has implications for the target detection algorithms and other data processing techniques that are employed. Three main functions are performed in a collision avoidance scenario, detection (monitoring), control and decision-making. Detection refers to the ability to identify, extract, track and estimate some attributes from the conflicting target in the field of view of the sensor. This information is then used by the control task to generate commands and perform the avoidance maneuver. Finally, decision-making uses instantaneous or historical information of the target to declare a collision, and in this case propose the most adequate resolution by determining the appropriate maneuver.

Physical System Requirements for Sense-and-avoid

The detection previously mentioned can be performed with a number of active or passive sensors. In this paper, we consider passive electro-optical (EO) sensors for detection. EO sensors offer a unique combination of features that make them attractive for collision avoidance such as passive, compact, light, low power, and high speed. Their maturity is at a stage that allows them to be operationally feasible even in relatively small UAS platforms with conservative SWaP budgets. The system architect must trade-off the desired detection range for a given intruder size, image resolution, lens field of view, image processing rate and false-alarm rate to arrive at the required SWaP footprint for the air vehicle. This trade off is discussed in detail in [6].

In an avionics context, the main requirement to consider in an EO sensor is the interface (data and power). This has an impact in the power bus and communication with the main processor. The use of modern digital data-busses such as IEEE 1394B or Gigabit Ethernet [7] is the best choice in terms of reusability, modularity and supportability.

Another important factor is the availability of the aircraft state to the collision avoidance payload. This information is used for control purposes or sensor data conditioning (e.g image stabilization[2]). This data should be available on a common data-bus to all modules. In instances where an end-to-end system is developed, the capability of issuing avoidance commands from the payload will depend on a suitable interface with the aircraft autopilot, in most cases through the Flight Management System (FMS), however a direct command path is also desirable to minimize delay in time-critical scenarios, or in the case of an FMS failure. Typical hardware interfaces used for this purpose includes RS232/422/485, CANBus and Ethernet. Aerospace standards for these interfaces are published and in-use in modern airliners like the Boeing 777 and Airbus A380 [8]. Interfaces based on a common bus (such as CANAerospace, ARINC-825 or the various Ethernet based standards such as ARINC 664) are often preferred over point-to-point links because of the low complexity and transparency when adding and removing nodes in the bus.

Certification Considerations

In order to certify a SAA system, the regulator (via industry bodies such as the RTCA) must determine the minimum performance standards and testing criteria. There are several potential approaches. One approach would be for the regulator to define hard requirements (prescriptive) of the SAA system detection and avoidance characteristics. Another approach would be to define the probability of a collision, given a collision course threat. The latter approach would allow the manufacturer to trade off the SAA system characteristics in light of the aircraft's speed, maneuverability, autopilot response times, in addition to the raw detection performance of the sensing system.

Whilst there has been lots of discussion and proposals generated world-wide surrounding technical standards for sense-and-avoid [5, 9], and work is ongoing within the RTCA [10], so far the only published standard is ASTM F2411 [11], although it has not yet been adopted as an approved standard by any National Airworthiness Authorities (NAAs). This standard specifies the required detection performance in terms of a minimum miss distance of 500' (152m). The system designer would

[2] Often image stabilization is performed using information from an inertial sensor directly attached to the EO sensor.

then have to determine the required detection range given the aircraft's performance characteristics in order to meet the miss-distance requirement. This standard fails to identify a false alarm rate, however as discussed below this may be intentional in order to provide some flexibility given operational or mission requirements. False alarms are not in themselves safety failures, however a high false-alarm rate would impact mission effectiveness, reduce the operator's confidence in the system, and therefore impact upon the system dependability.

Researchers at ARCAA have attempted to produce some metrics which may be used to define the performance characteristics of a particular SAA algorithm, which trades off spatial resolution of the vision system against detection range, allowing different systems to be more easily compared [6, 12, 13]. Results from this testing has demonstrated practical detection ranges in the order of 1-2km in real time, and with reasonable false alarm rates. There is no known published information on an equivalent human false alarm rate. The target false alarm rate should be set low enough so as not to be a nuisance, however must be traded off against the desired detection range. We propose that a target false alarm rate in the order of 0.1-1 per flight hour would be acceptable in Class G airspace in Australia. Airspace with higher traffic density or differing mission profiles may need to adopt different false alarm rates. This topic is the subject of further investigation.

Automated Emergency Forced Landing

Safe Emergency Landing is a critical function that is typically triggered by an unscheduled event in flight [14-16]. Is most commonly attributed to an engine failure, loss of high-level functions such as navigation or adverse weather. State-of-the-art automated navigation systems already exist for UAS, however there is a lack of automation in scenarios where the aircraft experiences an emergency situation. To date, the most commonly employed method to mitigate the severity of a UAS forced landing is the use of parachutes or parafoils to retard the rate of descent, while still providing some degree of controllability for the aircraft. Whilst this concept is attractive in that it still enables limited vehicle controllability even when both the engine and control surfaces have failed, it is highly susceptible to wind gusts and other atmospheric effects that may adversely affect the final impact point. Our approach is based on the premise that the UAS have still some degree of flight control so that the aircraft is able to maneuver to a desired landing site. In this sense, we define four main functions that must be performed during an emergency landing such as navigation, monitoring, decision-making and control.

Required functionalities in an emergency landing scenario

The emergency-landing process can be broken down into distinct stages, each having a separate function [14, 16]. Stage 1 is site selection which involves determining the best possible space to attempt a landing, considering factors such as the size of the area, its shape, ground slope, surface type and obstacles, and proximity to civilization. Environmental factors such as the wind direction and possible low-level turbulence are also important considerations. Detection of a landing area can be achieved by monitoring the environment with an onboard sensor. Stage 2 requires planning a path to the selected site that the aircraft can be guided along. Stage 3 involves final approach guidance to landing, which could involve last-second obstacle avoidance. At any time, the system may be required to jump back to a previous stage if the desired state cannot be achieved. Stage 2 and 3 includes functions such as navigation, control and decision-making.

Each main function previously mentioned can be typically associated with a given sensor(s). For instance, site-selection is most obviously based on a visual scan of the terrain in the immediate vicinity of the aircraft, and the obstacle-avoidance capability is similar to the detection function in a collision avoidance system. Therefore, a reasonable choice considering reusability and modularity, would be to use EO sensors for monitoring the terrain for possible landing areas. Once again, the selection of a suitable interface for sensors will allow seamlessly integration with the image-processing module. In this case, a digital interface for the EO sensor will greatly benefit the software support and reusability.

Navigation, decision-making and control functions involved in stages 2 and 3, can be typically performed by the core processing computer or Flight Management System (FMS). These functions are closely related with the sense-and-avoid monitoring function in instances where the information acquired by the EO sensor is used to command in real-time the

aircraft. In particular, the task of commanding an aircraft to a landing site that has been visually detected by the EO sensor requires a real-time low-level link with the autopilot, furthermore it requires fast interfaces between the EO sensor and the image-processing module. Once again, the modern high-speed digital data-busses with direct command link to the autopilot discussed in the previous section are required.

For the emergency-landing function, the authors are not aware of any published or proposed certification standards. One of the outcomes of the current research effort will be to consider how regulators might certify such a safety system.

Similar functional requirements between applications

The application or tasks considered in this paper share some of the critical functions in any aircraft. Navigation, monitoring, decision-making and control are generic functionalities that, to some extent, are present in any autonomous aircraft. Therefore, seems logical to integrate these functions by the use of common hardware and software design approaches. We describe next these functions in the context of the two applications studies.

Navigation: Traditionally referred as the estimation of the aircraft state [17], in this paper we refer to navigation as the ability of performing not only waypoint navigation but also construction and following of specific trajectories between waypoints, leaving the guidance of the aircraft to the control function. This capability is often referred as path planning, and may or may not account for terrain evasion. Simple planning strategies such as straight line between waypoints, loitering or coordinated flight are generally available in most autopilots. However when the planning task requires the use of more advanced algorithms [18], it entail the use of computers with FMS functions. In this case, a core processing computer can performs the planning task, while an interface with the autopilot allows the command and control of the aircraft from the core processing computer. Additionally, an interface with the image-processing computer will allow the dynamic re-planning of trajectories according with what the EO sensors are detection. For example, the collision avoidance system could command the aircraft by issuing commands to the FMS module to modify a pre-defined path.

Control: In this work, we define control as the task that is performed in the system that has direct access to the control surface actuators. Its main purpose is to stabilize the aircraft and command the motion of the aircraft between waypoints. This function is generally performed by an autopilot, and the way and level of interaction with external systems varies between manufacturers. For instances, there might be autopilot systems that allow access to the internal states of the control loops, and therefore allow external systems to issue desired values for the control loop. The level of interaction also refers to whether the autopilot allows access to the position, attitude or velocity control loops. The physical interface to access the autopilot also varies between vendors, but undoubtedly, the use of a common bus will permit seamless integration with the payload and/or the core processing computer, adding important capabilities such as complex path planning and sensor-based control.

Monitoring: This function plays a critical role in the applications considered in this paper. By monitoring the environment the aircraft is able to gain situation awareness as well as gather information necessary to perform its task. By using EO sensors with similar interfaces, this function can be performed in a single image-processing module, and by switching the core software task and the sensor[3], we can enable the capability of sensing other aircraft in the airspace or perform an controlled emergency landing in case of an onboard failure.

Decision-making: Is defined as the capability to assess multiple attributes or variables in order to achieve a single or multiple objectives. Whether the system is performing collision avoidance or forced landing tasks, this process can be executed in the same core processing computer, nonetheless making use of different sensors each of them with common interfaces. This approach would facilitate a switching strategy where the core software task in charge of the decision making process in each task, could be enabled or disabled on demand.

---

[3] In most cases EO sensors that are attached to a common digital interface can be enabled or disable by simply software commands.

Requirements for a common avionics architecture from the safety and risk perspective

Whilst the physical and functional requirements for the architecture are important, it is also critical to derive requirements for the design from the perspective of safety and risk mitigation, so that regulators can certify the system for use in civil airspace. In this section we apply the concept of the Aircraft Certification Matrix (ACM) to help define the system Development Assurance Levels (DAL) and architecture requirements in accordance with acceptable risk criteria.

Aircraft Certification Matrix

The Aircraft Certification Matrix (ACM) concept has been proposed as a way of systematically identifying airworthiness requirements for a given system based on its intended operational environment [19]. This approach can be compared with the classical Part 23/25 certification requirements combined with the Part 91/121 operational rules and equipage requirements for different intended uses of a particular aircraft system. The ACM makes the relationship between operating environment and equipment & certification requirements explicit.

Figure 1 is a simplified version of the ACM presented by Clothier et al [19]. The columns of the matrix represent different UAS type categories. This paper does not attempt to provide a new framework for categorization of UAS types, as the classifications schemes are under continuous discussion. In this paper we simply adopt three type categories to illustrate our example.

		Air Vehicle Classification		
		Type 1	Type 2	Type 3
Operating Area Classification	Cat X	Cert 0	Cert 0	Cert 0
	Cat A	Cert 0	Cert 1	Cert 2
	Cat B	Cert 1	Cert 2	Cert 3
	Cat C	Cert 2	Cert 3	Cert 4

Figure 1: Example Aircraft Certification Matrix

For illustration purposes, the types could be designated by weight and/or kinetic energy limits, for example:

- Type 1 – Small UAS (<25kg, < 30 kts)
- Type 2 – Medium UAS (<150kg, < 100kts)
- Type 3 – Large UAS (> 150kg)

The rows of the matrix represent operating environments. There would normally be several matrices each representing a different aspect of the operating environment. For the emergency landing system, we are concerned about the ground environment we are operating over, and once again we adopt four categories in order to illustrate our example. Analysis for the sense-and-avoid system would likewise adopt categories for the applicable airspace environment.

- Cat X – Unpopulated
- Cat A – Sparsely Populated
- Cat B – Moderately Populated
- Cat C – Densely Populated

Finally, the cells of the matrix represent the certification categories, in this case 0 through 4. Certification Category-0 corresponds to the 'zero risk' or 'don't care' category. Certification Category-4 corresponds to an operation where an accident could result in multiple human fatalities in a densely populated area such as a major city.

This brings us to a discussion of the different types of airworthiness requirements that would need to be considered for each certification category. In this case, we consider airworthiness in a global sense – i.e. all of the elements that contribute to an airworthiness system.

- Basic airworthiness judgment
- Approved Design Standards
- Conformity Verification
- Equipage Requirements
- Operational Requirements
- Maintenance Requirements
- Accident and Incident Investigation
- Regulatory Compliance

Figure 2 proposes an example scheme for different types of airworthiness requirements to be imposed on a particular operation. Justification for particular

scrutiny in any given area is required, and this would normally be the domain of the NAA.

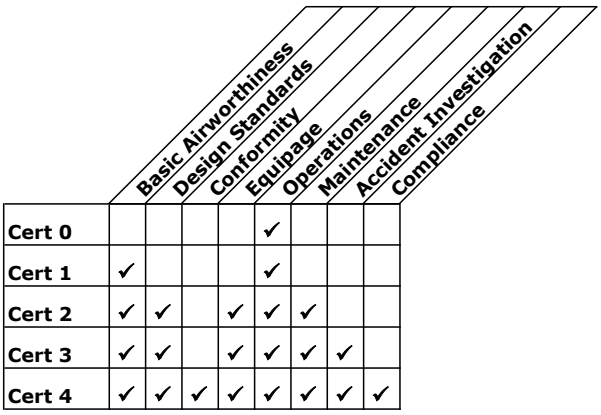

Figure 2: Example Airworthiness Certification Allocation

This discussion is important because it informs the adoption of a particular system architecture for a given operational scenario, and more importantly how a common architecture can be adapted to the different certification requirements.

Flight Guardian falls under the categories of Design Standards, Conformity Verification and Equipage. Design standards and conformity in the sense that the architecture is standards based and verified against those standards, and equipage in the sense that it includes specific functional capabilities to mitigate against particular failure conditions. So the principal application of Flight Guardian is for Category 2 to 4 operations, where the uptake of UAS is currently hindered by a lack of technology, standards and guidance.

Assignment of Development Assurance Levels

SAE ARP4754 [20] provides guidelines for assigning development assurance levels from the aircraft functional level through to the developmental item level. Development assurance is the process that establishes confidence that system development has been conducted to minimise the likelihood of errors that could impact safety.

The high-level functional requirements are summarized as:

F1. The UA shall be able to sense other aircraft in order to prevent a collision;
   a. Observe the environment and sense collision course aircraft;
   b. Decide on the best course of action to evade a detected collision course aircraft;
   c. Execute the avoidance action;

F2. The UA shall be able to perform a forced-landing in the event of an aircraft failure preventing continued safe flight and landing, where the aircraft remains controllable (i.e. propulsion failure);
   a. Determine a suitable landing site;
   b. Guide aircraft to landing site;
   c. Perform final approach obstacle avoidance to landing;

ARP4754 is designed for application to conventionally piloted aircraft, and therefore care must be taken when interpreting this guidance in the context of UAS. In particular surrounding the failure condition classifications (defined in [21]) that focus heavily on the effect of the failure on the operating crew and how they might be able to deal with a particular failure. In the case of an autonomous UAS where there is no crew to consider, the effect must be considered in terms of third parties. Nevertheless, the guidance provided in this standard for determining DALs is still very useful.

The traditional application of ARP4754 would now call for the system-level Functional Hazard Assessment. Table 1 lists the failure condition classifications from the existing guidance and relates them to the suggested ACM classes from Figure 1. For example, the functional failure of the emergency-landing function for a large-UAS over densely populated area could result in multiple human fatalities. At the other end of the scale, a Small UAS operating in a moderately populated area (ACM Class 1) could result in physical discomfort to 3rd parties if an engine failure resulted in the UAS hitting a house. Note that whilst more severe injuries could occur, the most likely outcome is used to assess the classification. Small UAS operating in sparsely populated areas, or all UAS operating in unpopulated areas are assumed to have no safety effect.

Table 1: Failure Condition Classifications

Classification	Effect	ACM Class	Nom. DAL
Minor	Physical Discomfort	1	D
Major	Physical Distress or Injury	2	C
Hazardous	Serious or fatal injury	3	B
Catastrophic	Multiple fatal injuries	4	A

Application of the standard allows for consideration of the probability of emergency conditions when determining the DAL. So the designer can now consider the probability of requiring the sense-and-avoid or emergency landing function. For example, if the P(emergency landing) < 10^{-5}, a Level A requirement can be reduced to Level B. Table 2 presents a suggested mapping of the certification categories to DALs based on this guidance.

For the loss of function failure condition, *Flight Guardian* must make a real-time assessment of the current operating conditions to determine if the flight can proceed. If the system were operating as a Cat 4 flight, the flight should be re-planned to a lower level in order to mitigate the reduction in safety margin caused by the failure.

Table 2: Mapping of Certification Category to DAL

Cert Cat	Nom. DAL	P(event) < 10^{-4}	P(event) < 10^{-5}	P(event) < 10^{-7}
0	E	E	E	E
1	D	E	E	E
2	C	D	D	E
3	B	C	C	C
4	A	A	B	C

The mappings for certification categories 3 and 4 are derived directly from ARP4754. However there is no guidance provided for the lower risk levels associated with categories 1 and 2. We have extrapolated the reductions in DAL from categories 3 and 3 into categories 1 and 2. In any case, the risk posed by categories 1 and 2 are much lower, and the principal application for *Flight Guardian* will be in category 3 and 4 operations.

For events with sufficiently low probability, such as mid-air collision [9], a DAL of B or C would seem to be suitable. This is consistent with the DAL requirement for TCAS-II, which is also level B. Similarly for the emergency forced landing function, a DAL commensurate with the event probability is appropriate. The designer would need to take into account several external and operational factors when determining the probability of impact with a densely populated area.

Application of ALARP

The ALARP ("As low as reasonably practicable") concept seeks to provide a framework for assessing the acceptability of risks relative to the status quo and reducing risks to tolerable levels through mitigation strategies, taking into account a reasonable cost of risk reduction [22]. The benefits of this approach are obvious at the high-level system of systems architecture development, where subjective societal issues and risk perception dominate the decision process. ALARP provides the framework for determining whether or not the inclusion of a particular risk mitigation strategy is worth the cost of implementation. However, there are several challenges to applying ALARP in a systematic and objective manner at the lower levels of complex hardware and software development [23, 24]. Investigation into this method should be the subject of further investigation.

Conclusion

In this paper, we presented an approach to derive requirements for the Flight Guardian system architecture. We examined common features between onboard functions in this architecture to propose certain guidelines in the design of the system. Furthermore, we assessed the safety, dependability and risk to derive requirements using an Aircraft Certification Matrix to define the system Development Assurance Level (DAL). Flight Guardian provides a unified sensing and processing architecture enabling sense-and-avoid and automated forced landing functions for an UAS.

The certification approach applied in this work allows the designer to determine the required level of system development assurance for the *Flight Guardian* system. This allows system architects the flexibility in configuring *Flight Guardian* for a particular operational profile (certification category). Therefore the implementation cost and certification burden is commensurate with the safety risk posed by the particular operation.

References

[1] US-DoD, "Unmanned systems integrated roadmap FY2011- 2036," Office of the Secretary of Defence2011.

[2] M. T. DeGarmo, "Issues concerning integration of unmanned aerial vehicles in civil airspace," MITRE Corporation2004.

[3] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing,* vol. Vol. 1, pp. 11-33, 2004.

[4] V. D. Florio, "Dependability and Fault-Tolerance: Basic Concepts and Terminology," in *Application-Layer Fault-Tolerance Protocols*, ed Hershey, PA: IGI Global, 2009.

[5] T. Hutchings, S. Jeffryes, and S. Farmer, "Architecting UAV Sense & Avoid Systems," presented at the IET Conference on Autonomous Systems, 2007.

[6] J. S. Lai, J. J. Ford, L. Mejias, A. L. Wainwright, P. J. O'Shea, and R. A. Walker, "Field-of-view, detection range, and false alarm trade-offs in vision-based aircraft detection," presented at the International Congress of the Aeronautical Sciences 2012.

[7] M. Norris, *Gigabit Ethernet Technology and Applications*: Artech House, 2002.

[8] ARINC. (2012). *ARINC Specifications*. Available: **http://www.arinc.com**

[9] J. N. Simon and M. S. Braasch, "Deriving sensible requriements for UAV sense-and-avoid systems," presented at the IEEE/AIAA 28th Digital Avionics Systems Conference, 2009.

[10] RTCA. (2012, 1 August 2012). *RTCA SC-203 Home Page*. Available: **http://www.rtca.org/comm/Committee.cfm?id=45**

[11] ASTM, "F2411-07: Standard Specification for the Design and Performance of an Airborne Sense-and-Avoid System," ed. Pennsylvania, USA: ASTM International, 2007.

[12] J. Lai, J. Ford, L. Mejias, P. O'Shea, and R. Walker, "Detection versus false alarm characterisation of a vision-based airborne dim-target collision detection system," presented at the 2011 International Conference on Digital Image Computing Tecniques and Applications, Noosa, QLD, 2011.

[13] L. Mejias, J. Lai, J. Ford, and P. O'Shea, "Demonstration of closed--loop airborne sense--and--avoid using machine vision," *IEEE Aerospace and Electronic Systems Magazine,* vol. Vol. 27, pp. 4-7, 2012.

[14] P. C. Eng, L. Mejias, R. A. Walker, and D. L. Fitzgerald, "Guided chaos: path planning and control for a UAV-forced landing," *IEEE Robotics and Automation Magazine,* vol. Vol. 17, pp. pp. 90-98, 2010.

[15] L. Mejias and P. C. Eng, "Experimental validation of an unpowered unmanned aerial system : application to forced landing scenarios," presented at the Digital Proceedings of the 2012 International Conference on Unmanned Aircraft Systems (ICUAS'12) 2012.

[16] L. Mejias, D. L. Fitzgerald, P. C. Eng, and X. Liu, "Forced landing technologies for unmanned aerial vehicles : towards safer operations," in *Aerial Vehicles*, L. T. Mung, Ed., ed Kirchengasse, Austria: In-Tech, 2009, pp. pp. 415-442.

[17] M. Kayton and W. R. Fried, *Avionics Navigation Systems.* : John Wiley & Sons, 1997.

[18] A. Tsourdos, B. White, and M. Shanmugavel, "Cooperative path planning of unmanned aerial vehicles," *AIAA Progress in Astronautics and Aeronautics,* vol. Vol. 255, 2011.

[19] R. A. Clothier, J. L. Palmer, R. A. Walker, and N. L. Fulton, "Definition of an airworthiness certification framework for civil

unmanned aircraft systems," *Safety Science,* vol. Vol. 49, pp. pp 871-885, 2011.

[20] SAE, "ARP4754A: Guidelines for Development of Civil Aircraft and Systems," ed: SAE Aerospace, 2010.

[21] FAA, "AC 23-1309E: System Safety and Analysis for Part 23 Airplanes," ACE-100, Ed., ed: U.S. Federal Aviation Administration, 2011.

[22] HSE. (2012, 18 July). *ALARP Suite of Guidance*. Available: **http://www.hse.gov.uk/risk/theory/alarp.htm**

[23] G. E. Jolliffe, "Considerations of ALARP for Complex Safety Related Systems," presented at the 3rd IET International Conference on System Safety, Birmingham, UK, 2008.

[24] R. E. Melchers, "On the ALARP approach to risk management," *Reliability Engineering & System Safety,* vol. Vol. 71, pp. pp 201-208, 2001.

Email Addresses

Luis Mejias Alvarez, luis.mejias@qut.edu.au

Duncan Greer, d.greer@qut.edu.au